

This Page Is Inserted by IFW Operations  
and is not a part of the Official Record

## **BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning documents *will not* correct images,  
please do not report the images to the  
Image Problem Mailbox.**

## PATENT ABSTRACTS OF JAPAN

(11)Publication number : 08-273296  
 (43)Date of publication of application : 18.10.1996

(51)Int. CI. G11B 20/10  
 G09C 1/00  
 G09C 1/00  
 G11B 20/12  
 H04L 9/06  
 H04L 9/32  
 // H03M 7/30

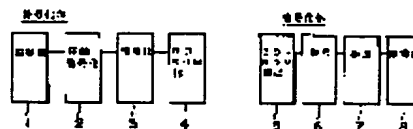
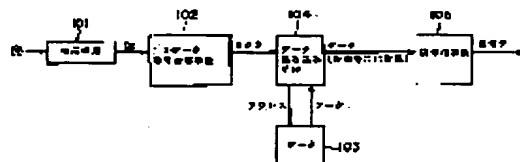
(21)Application number : 07-332358 (71)Applicant : FUJITSU LTD  
 (22)Date of filing : 20.12.1995 (72)Inventor : AKIYAMA RYOTA  
 YOSHIOKA MAKOTO

(30)Priority  
 Priority number : 06341068 Priority date : 29.12.1994 Priority country : JP

(54) DATA REPRODUCING SYSTEM, DISK RECORDING MEDIUM AND DATA REPRODUCING METHOD

(57)Abstract:

PURPOSE: To make possible reproduction, reverse reproduction, etc., of compressed-coded data from an arbitrary position by providing corresponding between ID and sectors for each block of sectors.  
 CONSTITUTION: An original dynamic image 1 is companding-coded by a circuit section 2 and ciphered 3 to be stored in a CD-ROM 4. A decoding section reads the data from the ROM 4 using a driving device 5 and decodes 6 it. The decoded data is expanded 7 and restored to the original dynamic picture 8. During this series of processing, an indicating means 101 and an ID-data number corresponding means 102 to which ID and the corresponding data number are registered are installed to perform reabout of data by a reading means 104 based on the data number obtained by the corresponding means 102 and the data is decoded by a means 105.



## LEGAL STATUS

[Date of request for examination] 29.08.2002  
 [Date of sending the examiner's decision]

of rejection]

[Kind of final disposal of application  
other than the examiner's decision of  
rejection or application converted  
registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's  
decision of rejection]

[Date of requesting appeal against  
examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998, 2003 Japan Patent Office

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平8-273296

(43) 公開日 平成8年(1996)10月18日

(51) IntCl. <sup>9</sup>	識別記号	庁内整理番号	F I	技術表示箇所
G 1 1 B 20/10		7736-5D	G 1 1 B 20/10	B
G 0 9 C 1/00	6 1 0	7259-5J	G 0 9 C 1/00	6 1 0 B
	6 6 0	7259-5J		6 6 0 D
G 1 1 B 20/12		9295-5D	G 1 1 B 20/12	
H 0 4 L 9/06		9382-5K	H 0 3 M 7/30	Z

審査請求 未請求 請求項の数10 O L (全 14 頁) 最終頁に続く

(21) 出願番号 特願平7-332358

(22) 出願日 平成7年(1995)12月20日

(31) 優先権主張番号 特願平6-341068

(32) 優先日 平6(1994)12月29日

(33) 優先権主張国 日本 (J P)

(71) 出願人 000005223

富士通株式会社

神奈川県川崎市中原区上小田中4丁目1番  
1号

(72) 発明者 秋山 良太

神奈川県川崎市中原区上小田中1015番地  
富士通株式会社内

(72) 発明者 吉岡 誠

神奈川県川崎市中原区上小田中1015番地  
富士通株式会社内

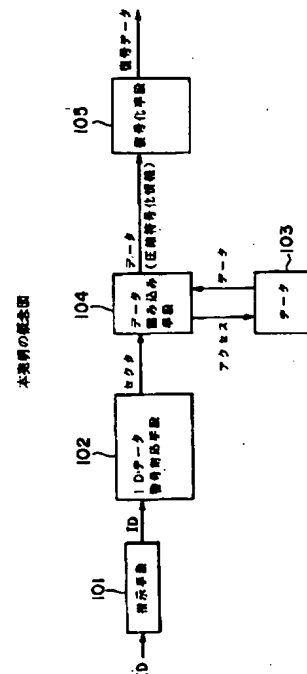
(74) 代理人 弁理士 遠山 勉 (外1名)

(54) 【発明の名称】 データ再生システム、ディスク記録媒体およびデータ再生方法

(57) 【要約】

【課題】 圧縮符号化(暗号化)されたデータについて  
ユーザーの所望する箇所からの再生(ランダムアクセ  
ス)や逆再生、さらにはスキップサーチを可能にする。

【解決手段】 暗号化された文字、画像、動画または音  
声などのマルチメディアデータを再生するシステムにつ  
いて、データのある程度のまとまり毎にIDを付与して  
このIDとCD-ROMのセクタとの対応付けを行うよう  
にし、前記IDを外部から指示することにより暗号化  
されたデータに対して直接セクタを指定したアクセスが  
できるようにした。



# 【特許請求の範囲】

【請求項1】 ブロック毎にブロック番号が付与された状態の入力データを再生するために出力するデータ再生システムであって、

少なくとも1つ以上のブロックで構成されるデータ列に付与されたID情報を外部より獲得するID獲得手段と、

前記ID情報とブロック番号との対応関係が登録され、前記ID獲得手段から指定されたID情報に対応するブロック番号を検出するID・ブロック番号対応手段と、前記ID・ブロック番号対応手段により得られたブロック番号に基づいて前記データの読み出しを指示する読出制御手段と、

前記読出制御手段により指示された読み出しデータの出力を制御する出力制御手段とからなるデータ再生システム。

【請求項2】 前記に加えて、暗号化または圧縮符号化された入力データを復号化する復号化手段と、前記復号化手段に対して暗号化または圧縮符号化されたデータを復号化するための個々の鍵情報とを有している請求項1のデータ再生システム。

【請求項3】 前記に加えて、前記鍵情報によって再生を許諾されたデータのフレームのID情報が登録される許諾情報管理手段を有する請求項1記載のデータ再生システム。

【請求項4】 前記に加えて、前記許諾情報管理手段に登録されたID情報と前記読み出しデータのID情報とを比較する比較手段を有し、前記出力制御手段は、比較手段からの一致情報に基づいて読み出しデータの出力を行う請求項3記載のデータ再生システム。

【請求項5】 前記に加えて、鍵格納手段を有しており、前記復号化手段は前記鍵情報を前記鍵格納手段から獲得する請求項2記載のデータ再生システム。

【請求項6】 前記に加えて、前記許諾情報管理手段には、課金情報が登録され、前記読み出しデータを出力する際に課金処理を行う課金処理手段を有している請求項3記載のデータ再生システム。

【請求項7】 前記に加えて、前記データへのアクセスはセクタ毎に付与されたセクタ番号でなされ、少なくとも一つ以上のセクタで構成されるフレーム毎にID情報が付与されており、これらのセクタ番号とID情報との対応関係を示す対応関係情報が記録された可換型記録媒体と、

この可換型記録媒体より前記セクタ番号とID情報との対応関係を示す対応関係情報を読み出す駆動装置と、駆動装置から読み出された対応関係情報を前記ID・ブロック番号対応手段に登録する初期化手段とを有している請求項1記載のデータ再生システム。

【請求項8】 情報格納領域が複数のセクタに分割さ

れ、前記セクタにはセクタ番号を記録するインデックス部と、データを記録する記録フィールドとからなり、少なくとも1つ以上のセクタで構成されるフレーム毎に付与されるID情報が前記インデックス部に記録されているディスク媒体。

【請求項9】 ブロック毎にブロック番号が付与されて入力されたデータの再生・出力を行うデータ再生方法であって、

少なくとも1つ以上のブロックで構成されるフレーム毎に付与されたID情報を獲得するステップと、

前記ID情報とブロック番号の対応関係を示す対応テーブルから、外部から指定されたID情報に対応するブロック番号を検出するステップと、

前記対応テーブルより得られたブロック番号に基づいて前記データの読み出しを行うステップと、

前記読み出しデータのID情報が予め出力の許諾を受けたID情報であるか否かを検査するステップと、

前記ID情報が許諾されたID情報であるときに、前記読み出しデータをデータ出力手段に出力するステップとを有するデータ再生方法。

【請求項10】 前記読み出しデータをデータ出力手段に出力するときに、課金情報を更新するステップを有する請求項9記載のデータ再生方法。

## 【発明の詳細な説明】

### 【0001】

【発明の属する技術分野】 本発明は、動画像データ等の圧縮符号化したデータを管理センタがCD-ROMあるいは通信データの形式で配信し、これを受け取ったユーザーが再生するための装置に適用する技術である。

### 【0002】

【従来の技術】 動画像データを圧縮するとともに暗号化してこれをCD-ROM等の大容量記録媒体に格納して配布する手順としては、以下のように処理が行われる。

【0003】 まず、動画像データの提供側（符号化部）では、原動画をまずMPEG等の規格で圧縮符号化部で圧縮符号化した後、これを暗号化回路で暗号化し、CD-ROMに格納する。

【0004】 そしてエンドユーザ側（復号化部）では、CD-ROMドライブ装置でこのCD-ROMからデータの読取りを行った後にこれをDES (Data Encryption Standard) で構成された復号部で復号する。この復号部は、たとえば「FIP'S PUB 46DATA ENCRYPTION STANDARD NIST」の規格のものをを用いることができる。

【0005】 この復号データはさらにMPEGデコーダ等の伸長部で伸長されて原動画に復号される。

### 【0006】

【発明が解決しようとする課題】 ところでCD-ROM形式で提供されたデータの場合、CD-ROMドライブ装置でのCD-ROMへのアクセスは実際にはセクタ単位に行われる。しかしデータが圧縮符号化されて格納さ

れている場合、ビットの並びが変化しているためいずれのセクタにどのようなデータが記録されているかを外部から認識することは容易ではなかった。

【0007】一方、通信回線を経由して得られたデータには本来的にセクタの概念が存在しない。この通信データを光磁気ディスク等に一旦蓄積した後に、これを再生することが考えられるがこの場合にも光磁気ディスクのどのセクタにどのようなデータが記録されているかを外部から認識することは難しかった。

【0008】このようにデータとセクタとの対応関係が不明なために暗号化されたデータが格納された媒体からのデータの再生では、ユーザーが望む任意のデータ位置からの再生（ランダムサーチ）や、高速早送り（スキップサーチ）、あるいは逆再生等のデータの特種再生が困難だった。

【0009】本発明は、このような問題点に鑑みてなされたものであり、ユーザーIDを設定してこのユーザーIDとセクタとを関連付けて管理するようにしたことにより、圧縮符号化（暗号化）されたデータについてユーザーの所望する箇所からの再生（ランダムアクセス）や逆再生、さらにはスキップサーチを可能にした。

【0010】なお、CD-ROMドライブ装置の内部構成を示したものとしては、特開平6-12785号、特開平1-21760号、特開平1-21761、特開平5-307592号、特開平5-313826号公報等がある。

#### 【0011】

【課題を解決するための手段】本発明は、すくなくともブロック毎（セクタ毎）に付与されたID情報を外部から獲得するID獲得手段を設け、ID情報とブロック番号との対応関係を示す対応テーブルを参照して前記ID情報に対応するブロック番号を検出するID・ブロック番号対応手段を設け、読出制御手段によって前記ID・ブロック番号対応手段により得られたブロック番号に基づいて前記データの読み出しを指示するとともに出力制御手段で前記読み出しデータの出力を制御するようにした。

【0012】すなわち、ハードウェアによるデータへのアクセスは実際にはブロック単位（セクタ単位）で行われるが、これらのブロック（セクタ）のまとまり毎にIDを付与してIDとブロック（セクタ）とを対応付けることにより圧縮符号化されたデータに対して任意の位置からの再生や逆再生等が可能となる。

【0013】なお、前記復号手段に対して暗号化または圧縮符号化されたデータを復号化するための鍵情報を外部より与えるとともに、再生を許諾されたID情報を登録するための許諾情報管理手段を設けても良い。

【0014】また、前記データをCD-ROM（Compact Disk Read-Only Memory）等の可換型記録媒体に記録してこの媒体中にセクタ番号とブロック（たとえばフレ

ーム）毎に付与されたID情報との対応関係を記録しておき、媒体の駆動装置からこれらの対応関係を読み出して、この対応関係のデータによってシステムに設けたID・ブロック番号対応手段を初期化してもよい。

【0015】なお、本発明において、データはCD-ROM、光磁気ディスクまたは磁気ディスクを例に説明しているが、これに限られず通信路を経由して得られるデータであってもよい。またデータの種類も動画像、静止画、音声、プログラム等いかなるデータ形式であってもよい。

【0016】また、IDを外部から獲得するための構成としては、たとえば赤外線送信部を設けた外部リモコンと、赤外線受信装置との組み合わせによるハードウェアを用いることができる。このシステムの具体的な使用例としては、たとえば映画毎または特定のシーン毎にIDが付与されており、ユーザーはそのID番号をリモコンを通じて指定することができる。

【0017】復号化手段は、DES（Data Encryption Standard）などの復号回路で構成されている。本発明では、CD-ROMなどの記録媒体上に圧縮符号化されて記録された動画像データに対して、ユーザーは外部からIDを指定してやるだけで任意の画像を再生することができる。指示手段を通じてIDが入力されると、ID・ブロック番号対応手段はこのIDを記録媒体上のセクタ番号に変換する。このセクタ番号に基づいて出力制御手段はCD-ROM上の所定のデータ箇所にアクセスしてデータの読み出しを行う。そしてこのデータは復号化手段において復号されてビデオ信号等に変換されてCRT等に表示される。

【0018】このように、CD-ROM上に記録された圧縮符号化データについて、ある程度のまとまり毎にIDを付与して管理してやることにより、このIDを基準にして再生開始、スキップサーチを実現できる。

【0019】なお、IDはセクタ単位に付与されてもよいが、一定数のまとまりのあるセクタに対して付与されることが好ましい。また、一つのIDが付与されるセクタ数はかならずしも同数である必要はなく、映画等のシーン毎のように複数のセクタのまとまり毎に単一のIDが付与されてもよい。

【0020】さらにデータが通信回線を経由して得られた場合には、ヘッダに対する一定長のペイロード毎にIDを付与してもよい。この場合にはIDはデータの一定長毎に記録されることになるのでIDの検出を同期信号とすることができる。

#### 【0021】

【発明の実施の形態】本発明の概念を図1および図2に基づいて説明する。図1は本発明によるデータ再生システムの処理を概念的に示しており、図2は本システムを符号化および復号化の処理に分けて示している。

【0022】図2に示すように、動画像データの提供側

(符号化部)では、原動画1をまずMPEG等の規格にしたがって圧縮符号化部2で圧縮符号化した後、これを暗号回路3で暗号化し、CD-ROM4に格納する。

【0023】そしてエンドユーザ側(復号化部)では、CD-ROMドライブ装置5でCD-ROM4からのデータ読み取りを行った後にこれをDES(Data Encryption Standard)等の復号部6で復号する。この復号部6は「FIP'S PUB 46DATA ENCRYPTION STANDARD NIST」の規格のものが採用されている。

【0024】この復号データはさらにMPEGデコーダ等の伸長部7で伸長されて原動画8に復元される。このような一連の処理を通じて、本発明では図1に示すように指示手段(101)を設け、IDとこれに対応するデータ番号とが登録されたID・データ番号対応手段(102)を設け、このID・データ番号対応手段(102)で得られたデータ番号に基づいてデータ読込手段(104)によってデータの読み込みを行い、復号手段(105)において復号化するものである。

【0025】図3はデータを供給する側で用いられる符号化装置の回路構成を示すブロック図である。同図において、前処理部14は、原データをデジタル化する機能を有している。次段の圧縮符号化部2は、デジタル化された動画像データをMPEGの規格に基づいて圧縮する機能を有している。

【0026】第1バッファ15は、前記圧縮符号化部2で圧縮された動画像データ(圧縮符号化データ)を蓄積する。また暗号回路3は、圧縮符号化データを暗号化データに変換する機能を有している。なお、暗号回路3が実行する暗号化処理としては、動画像データの画像データのみを暗号化する方法、画像データと音声データの両者を暗号化する方法とがあるがいずれでもよい。

【0027】また、暗号処理は圧縮符号化された順序でブロック単位(フレーム単位)で行う。PID格納部19には、一定の動画像データのまとまり毎に付与されるPID(ペイロードID)が格納されており、このPID格納部19から読み出されたPID情報は、制御回路17によってヘッダ情報の一部として第2バッファ16に転送される。

【0028】第2バッファ16は、暗号化したフレーム動画像データを蓄積し、暗号化画像データ蓄積回路20は暗号化したフレーム動画像データを暗号化画像データとして組み立てる機能、すなわちヘッダとフレーム長情報と暗号化圧縮画像データとを1単位のフレームデータとして組み立てる機能を有している。

【0029】次に本実施の形態における処理手順を図4のフロー図に基づいて説明する。制御回路17はまず初期化処理(ステップ401)を実行する。この初期化処理については、図5のフローに示すように、まず第1バッファ15と第2バッファ16の内容をクリアする(ステップ501)。次に、暗号回路3をクリアしこの暗号

回路3に暗号鍵を設定してデータを暗号化するための暗号モードのロジックを決定する(504)。

【0030】以上のような初期化処理が完了すると、図4のフローに戻り圧縮符号化部2を起動する(402)。画像データはこの圧縮符号化部2によって圧縮符号化されて第1バッファ15に順次蓄積されていく(403)。

【0031】次に制御回路17は、PID格納部19よりPID情報を読み出してフレーム毎のヘッダ情報を生成してこれを第2バッファ16に転送しておく(406)。次に前記第1バッファ15から読み出された画像データは暗号回路3で順次暗号化され(408)、1フレーム分の処理が完了すると順次第2バッファ16に暗号化データとして書き込まれる(409)。

【0032】このような1フレーム分の暗号化処理が完了すると(410)、第2バッファ16はその1フレーム分の暗号化データを暗号化画像データ蓄積回路20に出力する。

【0033】そして、これに続く次の1フレーム分のデータが第1バッファ15から読み出されて前述の処理が繰り返される。前述の暗号処理において、暗号回路3は高速かつ安全(鍵情報なくして解読不可能)なアルゴリズムを用いる。たとえば米国標準暗号であるDES(Data Encryption Standard)やFEAL(Fast Encryption Algorithm)、IDEA(International Data Encryption Algorithm)などを用いるとよい。ただし、本発明ではフレーム長がビット単位で変化する可能性があるため、ブロック単位で処理する暗号方式を採用する場合には、暗号すべきデータがブロック長に満たないときにはその部分の暗号化は行わない等の工夫をする必要がある。

【0034】ブロック長データに満たない部分データの処理としては、決まったビットパターンを1ブロック長となるまで挿入してもよい。また、CBCモードとKビットCFBモード(Kビットは余った暗号ビットを意味している)とを併用してもよい。この方式を採用する場合、CFBモードの初期ベクトルはCBCモードの最終値とする。さらに、64ビットOFBモード、1ビットOFBモードまたは1ビットCFBモードのいずれかで処理する方法もある。

【0035】またCBC、OFB、CFBモードで必要となる暗号化のための初期ベクトルとしてフレームヘッダに含まれる時間情報やシーケンス番号を用いる方法もある。

【0036】本実施例において暗号化画像データ蓄積回路20によって組み立てが完了したフレームフォーマットを示したものが図6である。当該フレームフォーマットの1ブロックの構成は、ヘッダ13aとPID13bと暗号フラグ13dとで構成されるIDフィールドと、暗号化圧縮画像データ13cが格納されたデータフィー

ルドとからなる。このヘッダ13aには画像の伸長制御信号(同期信号)が記録されており、PID13bにはデータフィールドに記録された暗号化圧縮画像データのPID(ペイロードID)が記録されている。暗号フラグ13dにはデータフィールドに記録されたデータが暗号化されたものか否かを示すフラグが記録されている。このようなフォーマットのデータがCD-ROMに格納した状態で、または通信回線を経由してユーザに提供される。

【0037】図13は本実施例の再生装置の機器構成を示す説明図である。再生装置本体131にはCD-ROM122を装着可能なCDドライブ装置132と後述の復号モジュールを構成するSDカード135を装着可能なSDカードスロット133が設けられており、内部にはプログラムおよびデータを蓄積可能なハードディスク装置134が設けられている。

【0038】また、再生装置本体131の前面には赤外線信号受信部(OCR)が設けられており同図に図示していない赤外線リモコンからデータ再生のためのIDを受信可能となっている。

【0039】なお、暗号化データをCD-ROM122から複写するためのMOドライブ136を設けてもよい。このMOドライブ136には光磁気ディスク137やパーシャルROMディスク(一部が書き換え可能なROM媒体)を装着できるようになっている。

【0040】図7は前記再生装置の機能ブロック図である。インターフェース131にはハードディスクドライブ装置(HDD)、光磁気ディスクドライブ装置(MOD)、CD-ROMドライブ装置(CD-RD)およびモデム(MDM)が接続されており、磁気記録媒体、光磁気記録媒体、光記録媒体または通信データとして暗号化された圧縮符号化データを入力できるようになっている。

【0041】このような多様なデータ入力形式のうちCD-ROM122を用いる場合のドライブ装置111を示したものが図14である。ドライブ装置111はCD-ROM122に記録されたデータを読み取る光学式ピックアップ142を有しており、この光学式ピックアップ142で読み取られたデータは復調回路141で復調されてインターフェース131に対して暗号化データとして出力される。

【0042】ここで本実施例で用いられるCD-ROM122は、動画データが圧縮符号化(暗号化)された状態で記録されており、その一部にインデックス部分として画像データのPID(たとえば映画のシーン毎に付与されたID)とこれに対応するセクタ番号とが記録されている。すなわち、動画データはすべて暗号化されているため、通常の再生方法では全てのデータを復号化して再生してみなければどのセクタにどの部分のデータが格納されているのか分からない。そこで、本実施例で

は図15に示すように、CD-ROM122の一部にデータを識別するIDとセクタ番号とを対応付ける対応記録部151を設けている。この対応記録部151は当該CD-ROMがドライブ装置111に装着された初期状態でスキニングされてその内容が後述のセクタ番号PID対応ポインタテーブル117に複写されるようになっている。

【0043】DES112は、ドライブ装置111を通じてCD-ROM122から読み出された圧縮符号化データ(暗号化データ)を解読すなわち復号化する機能を有している。

【0044】図8はDES112の概略構成を示している。DES112は同図に示すように、DES実行部215を有しており、入力データ(IN)を鍵情報216で得られるアルゴリズムに基づいて復号して出力データ(OUT)として出力する機能を有している。

【0045】DES実行部215はモード識別部218を有しており、このモード識別部218は複数のDESモードの中からそのデータ形式によって最適なモードを選択してDES実行部215に与える機能を有している。

【0046】次に前記DESモードのうち、代表的なロジック回路を説明する。図9(a)は、ECB基本モードであり、DES実行部215において、64ビットの鍵情報216により64ビット入力データ列を64ビットの出力データ列として暗号化(または復号化)するモードである。

【0047】図9(b)は、CBCモードを示しておりDES実行部215において64ビットの入力データ列を64ビットの鍵情報216で暗号化(または復号化)した後、再度これをDES実行部215に帰還入力させる。このようにデータを全て入力し終えるまでフィードバックを行い最終結果を出力する方式であり、ファイル等のデータ処理に適している。

【0048】図9(c)は、OFBモードを示しており、エラーの生じやすい通信データや、一つのエラーが他に与える影響の大きい音声データ等の処理に適している。図9(d)は、CFBモードであり、自己同期形のデータ処理に適している。

【0049】前述のモード識別部218はモードテーブル220に格納されたこれらのモードのうちデータ形式等を解析して最適なものを読み出してDES実行部215に出力する。DES実行部215ではこのようにして選択されたモードに基づいて暗号化・復号化処理を行う。

【0050】図10は、DES実行部215のハードウェア構成を示すブロック図である。同図において、入力側には入力用バッファとして8ビット構成のレジスタが8個接続されて64ビットのシフトレジスタ(入力レジスタ221:REG1)が配置されており、次段には複



数のセクタ *se1* が配置されている。当該セクタ *se1* は、後述のDES処理メイン回路225からの出力か、前記シフトレジスタ221からの出力かを選択的に入力できるようになっている。

【0051】セクタ *se1* の次段には8ビット構成のレジスタ223 (REG2) が配置されてさらにその次段にはDES処理メイン回路225が配置されている。このDES処理メイン回路225がDES実行部215として機能する。すなわち、DES処理メイン回路225には、図9で説明した各種のDESモードがROMとして登録されており、制御装置113からの指示により最適なDESモードのロジックを選択して復号処理を行うようになっている。

【0052】前記DES処理メイン回路225の出力は前記セクタ *se1* と出力用バッファとしての出力レジスタ224 (REG3) に分岐されている。そして出力レジスタ224 (REG3) の出力が暗号化または復号化されたデータとして用いられる。

【0053】この処理のシーケンスを示したものが図11である。同図において、入力レジスタ221の出力は、次サイクルの最初のクロックでレジスタ223からの出力としてDESの処理がなされる。そして次のクロックで出力レジスタ224より出力される。この出力レジスタ224からの出力時間に入力側では入力レジスタ221より次サイクルの暗号化データの読み込みが行われている。

【0054】このように、本実施例では入力用バッファとしての入力レジスタ221と、出力用バッファとしての出力レジスタ224とを設けたことにより、暗号化データの入力と復号化データの出力とをそれぞれ独立して連続的に行うことができるようになった。そのため、従来のDESのようにサイクリックに入力と出力とを行う場合に較べて高速な復号化・暗号化処理が可能である。

【0055】課金テーブル114は、ユーザーがあらかじめ所定の方法で使用料を支払った動画像データ等のPIDとその使用料の残高が記録されている。この課金テーブル114とDES112とはたとえばICカード等にモジュール化して (SDカード135) 内蔵されており、ユーザーはこのSDカード135に直接アクセスすることはできないようになっている。ユーザーがSDカード135内の課金テーブル114のデータ内容を書き換えたいときにはSDカード135を販売店などに持参して所定の料金の支払う。その後、この販売店に設置された書換装置 (図示せず) で支払い料金に応じた残高値の更新、または許可PIDの追加登録ができるようになっている。

【0056】外部インターフェース回路120はID獲得手段として機能し、具体的にはキーボード (KB)、モデム (MDM)、マウス (MS) および赤外線受信装置 (OCR) 等が接続されている。このうち赤外線受信

装置 (OCR) を通じて外部リモコン (図示せず) よりIDを受信することができる。

【0057】外部インターフェース回路120から再生要求PIDを受け取ると、セクタ番号PID対応ポインタテーブル117が参照されて当該PIDに対応したセクタ番号が検出される。

【0058】図12はセクタ番号PID対応ポインタテーブル117のテーブル構成を示している。ドライブ装置111にCD-ROM122が装着されその対応記録部151が読み取られるとその読み取りデータがこのテーブル117に複写されて内容が更新されるようになっている。

【0059】テーブル117にはペイロードIDと各ペイロードIDに対応したセクタ番号が登録されるようになっている。外部からの再生要求PIDに基づいてセクタ番号PID対応ポインタテーブル117がアクセスされてセクタ番号が検索されると、制御装置113はドライブ装置111に対して当該セクタの読み出しを指示する。

【0060】読み出されたセクタに対応するデータは、まずIDフィールド解析部115でIDフィールドが解析される。IDフィールド解析部115は、DES112から読み出した復号データの中からIDフィールドを抽出してその中からPIDを抽出する。

【0061】比較器116は、前記IDフィールド解析部115で抽出されたPIDと、課金テーブル114から読み出されたPIDとを比較する機能を有している。すなわち、課金テーブル114において当該ユーザーに許可されているPIDとIDフィールド解析部115から抽出されたPIDとが一致するか否かが判定され、一致する場合にのみ比較器116はON信号をパケットスイッチ118に対して出力するようになっている。

【0062】パケットスイッチ118は、データ変換部121に対して出力するデータを切り換える機能を有しており、本実施例ではデータを出力しない状態、DESによって復号化されたデータを出力する状態および画像メモリ119に蓄積されたスチール画像を出力する状態のそれぞれに切換可能となっている。

【0063】データ変換部121はデジタル/アナログ変換器 (D/A変換器) で構成されており、CD-ROM122から読み出したデジタルデータをNTSC信号等のアナログ信号に変換するためのものであり、ディスプレイ装置 (DSP)、スピーカー (SP) またはインターフェース回路 (I/F) を介してプリンタ (PR) 等と接続されている。

【0064】本装置構成において、まずドライブ装置111にCD-ROM122が装着されるとブート状態となり、制御装置113の指示によりCD-ROM122の対応記録部151が読み出されてその内容がセクタ番号PID対応ポインタテーブル117に複写される。

【0065】当該CD-ROM122の再生時において、CD-ROM122から読み出された圧縮符号化（暗号化）された状態のデータブロックは、DES112で順次復号化される。

【0066】IDフィールド解析部115では、これらの読み出しデータを解析してPID13bを抽出し、このPIDを比較器116に通知する。これと並行して課金テーブル114からは再生が許可されているデータのPIDが比較器116に通知される。

【0067】比較器116では復号化されたデータのPIDが課金テーブル114で許可されているPIDと一致した場合にのみパケットスイッチ118を開く。これによってデータフィールドから読み出されてDES112で復号化されたデータがディスプレイ装置（DSP）を通じて出力される。

【0068】一方、比較器116での比較結果が不一致であった場合には、当該データは再生を許可されていないデータであるので、パケットスイッチ118はオフ状態となり、画像メモリ119に格納された静止画データ、たとえば注意を促す画像データがディスプレイ装置（DSP）を通じて出力される。

【0069】なお、赤外線リモコン（図示せず）を通じて外部インターフェース回路120よりPIDをインクリメントするコマ送り等の指示がなされたときにはセクタ番号をたとえば10セクタずつ加算してドライブ装置111への読み取りが指示される。これによってコマ送りによる高速な早送り動画像を実現できる。

【0070】また逆方向への動画像の再生、任意の位置からの動画像の再生もPIDを基準にして可能である。本実施例によれば、データをPIDで管理することとし、データが圧縮符号化（暗号化）して記録されたCD-ROM122上にこのPIDとセクタ番号との対応関係を記録したインデックス部を設け、再生装置側にこのインデックス部をそのまま複写可能なテーブルを設けアクセス時にはこのテーブルを参照してPIDからセクタ番号を検索可能にした。これによりデータが全て圧縮符号化されている場合にもPIDを識別基準としたランダムサーチや特殊再生を可能にした。

【0071】

【発明の効果】本発明によれば、ユーザーIDを設定してこのユーザーIDとセクタとを関連付けて管理するようにしたことにより、圧縮符号化（暗号化）されたデータについてユーザーの所望する箇所からの再生（ランダムアクセス）や逆再生、さらにはスキップサーチが可能となった。

【図面の簡単な説明】

【図1】 本発明の概念図

【図2】 動画像における圧縮符号化およびその復号化の処理を示す説明図

【図3】 実施例における符号化システムを示すブロック図

【図4】 実施例における符号化処理を示すフロー図

【図5】 実施例における制御回路の初期化処理を示すフロー図

【図6】 実施例のデータ構成を示す説明図

【図7】 実施例の圧縮符号化データ再生装置の構成を示すブロック図

【図8】 実施例におけるDESの構成を示すブロック図

【図9】 実施例におけるDESの各種モードを説明するための図

【図10】 実施例におけるDES実行部の高速化を図るための構成を示すブロック図

【図11】 実施例におけるDES実行部の処理シーケンスを説明する図

【図12】 実施例のセクタ番号PID対応ポインタテーブルの内容を示す説明図

【図13】 実施例の再生装置の機器構成を示す説明図

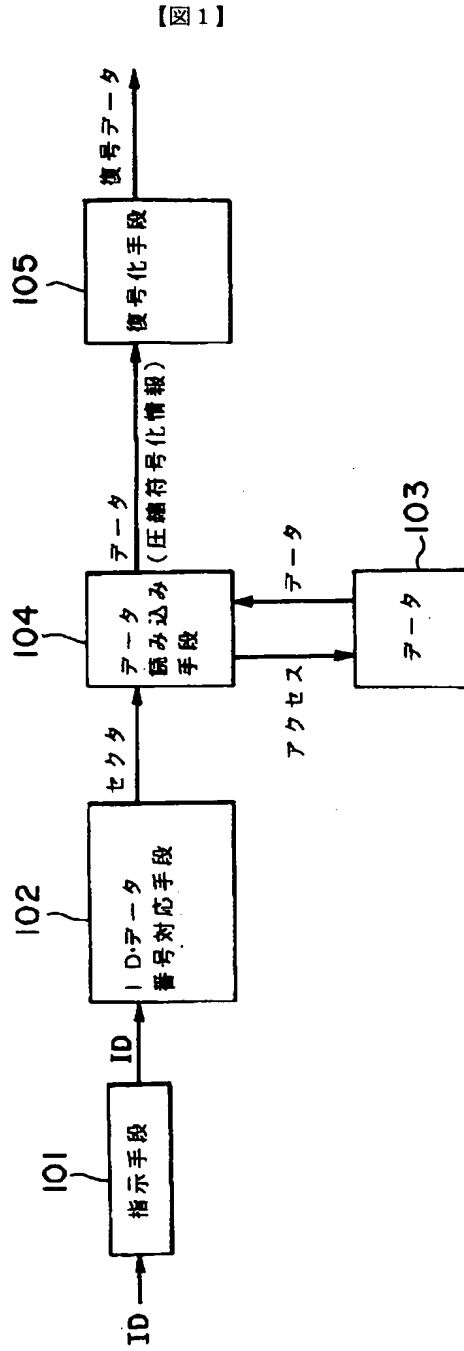
【図14】 実施例の再生装置に用いられるドライブ装置を示す図

【図15】 実施例のCD-ROM上の対応記録部の配置状態を示す図

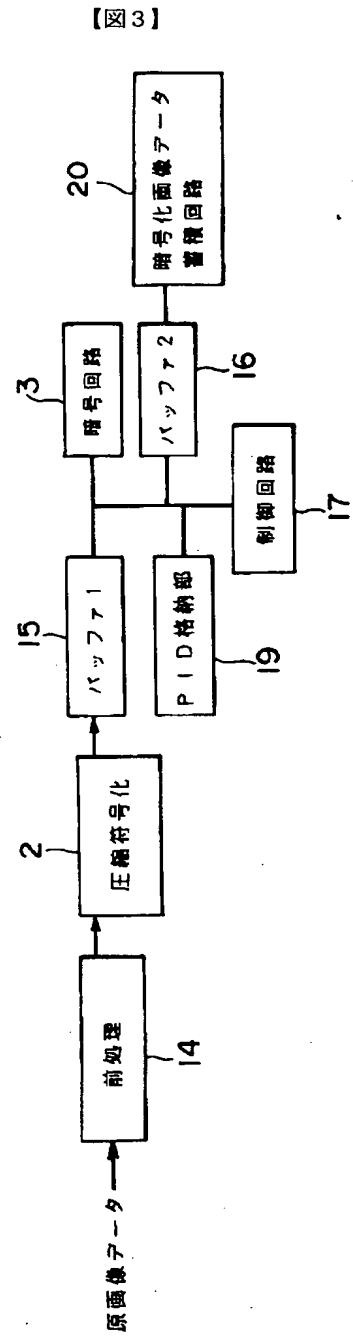
【符号の説明】

- 1・・・原動機
- 2・・・圧縮符号化部
- 3・・・暗号回路
- 4・・・CD-ROM
- 5・・・CD-ROMドライブ装置
- 6・・・復号部
- 7・・・伸長部
- 13a・・・ヘッダ
- 13b・・・PID
- 13c・・・暗号化圧縮画像データ
- 13d・・・暗号フラグ
- 14・・・前処理部
- 15・・・第1バッファ
- 16・・・第2バッファ
- 17・・・制御回路
- 19・・・PID格納部
- 20・・・暗号化画像データ蓄積回路
- 101・・・指示手段
- 102・・・ID・データ番号対応手段
- 104・・・データ読込手段
- 105・・・復号手段

本発明の概念図

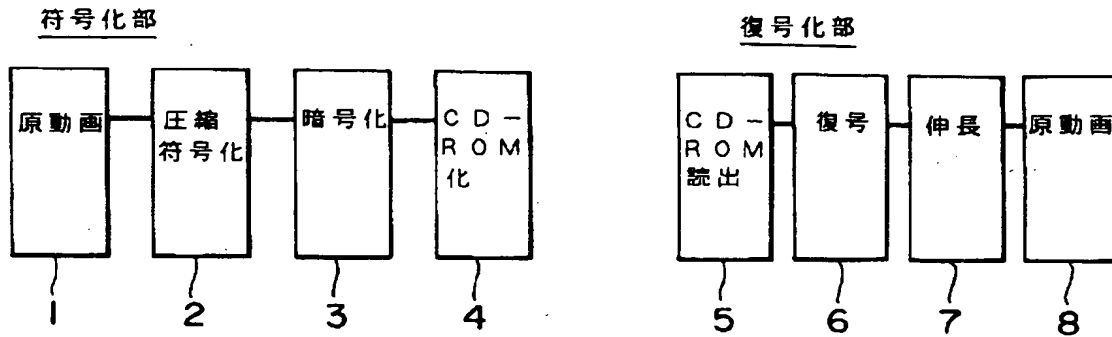


実施例における符号化システムを示すブロック図



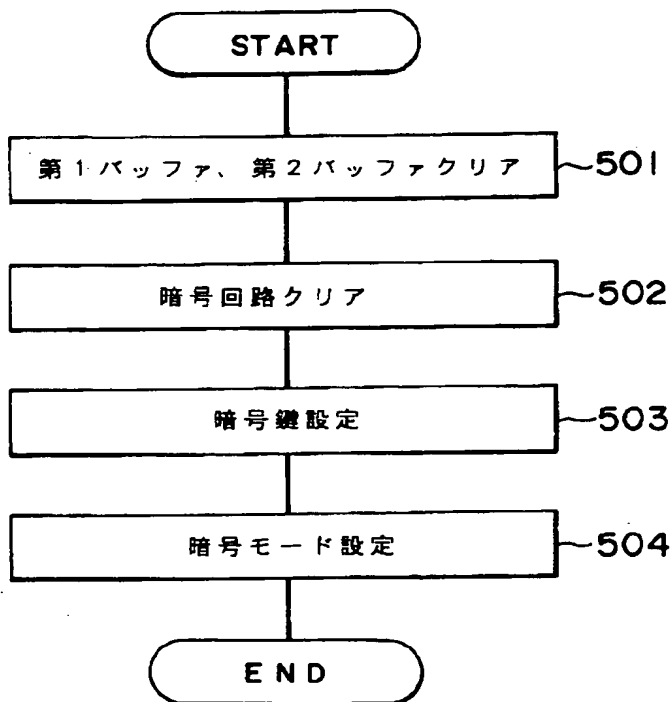
【図2】

動画像における圧縮符号化およびその復号化の処理を示す説明図



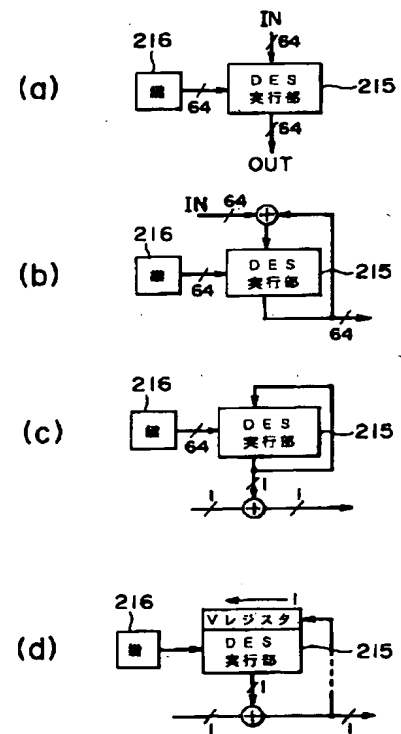
【図5】

実施例における制御回路の初期化処理を示すフロー図



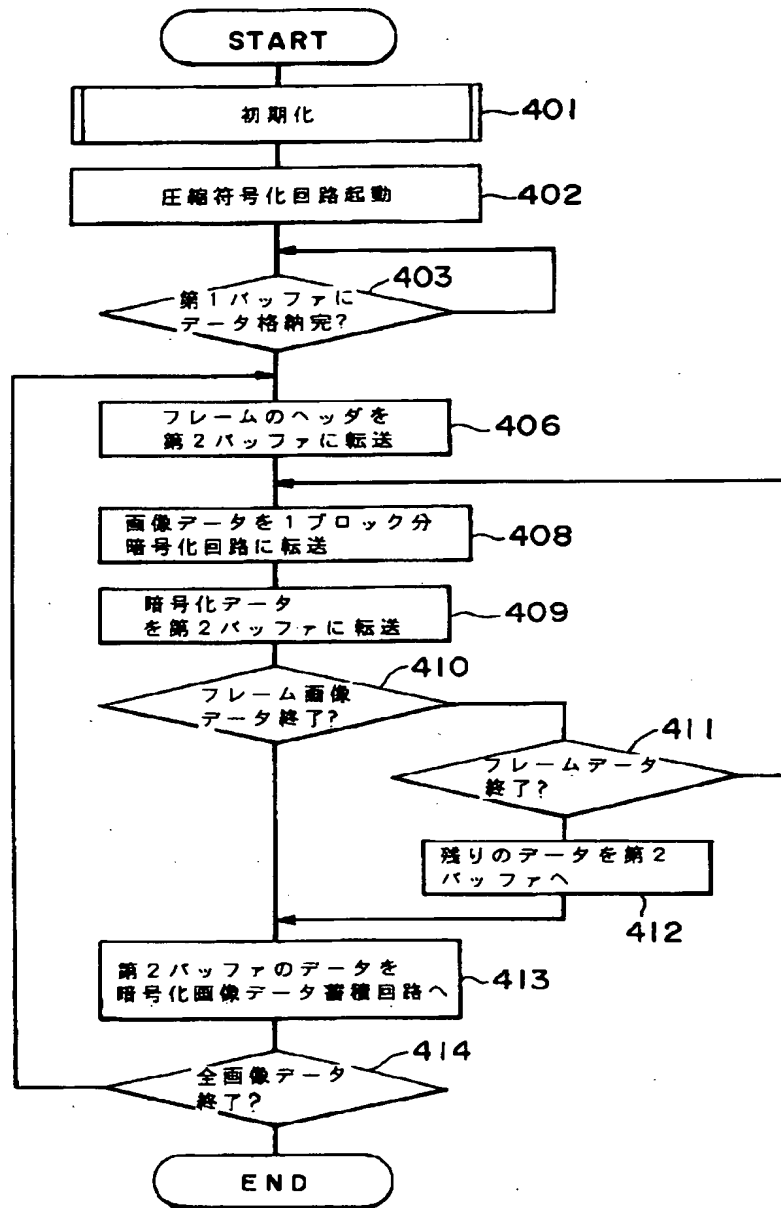
【図9】

実施例におけるDESの各種モードを説明するための図

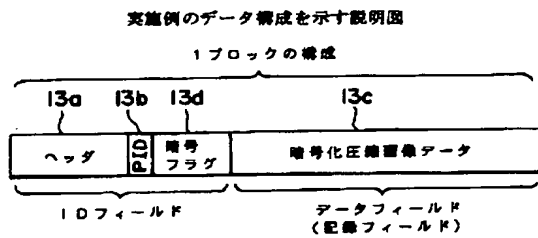


【図4】

実施例における符号化処理を示すフロー図

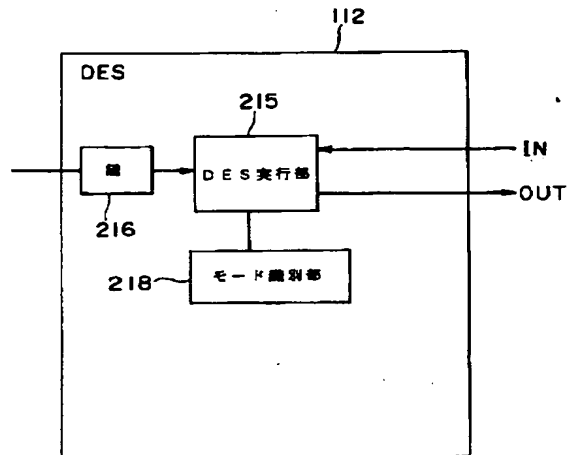


【図6】



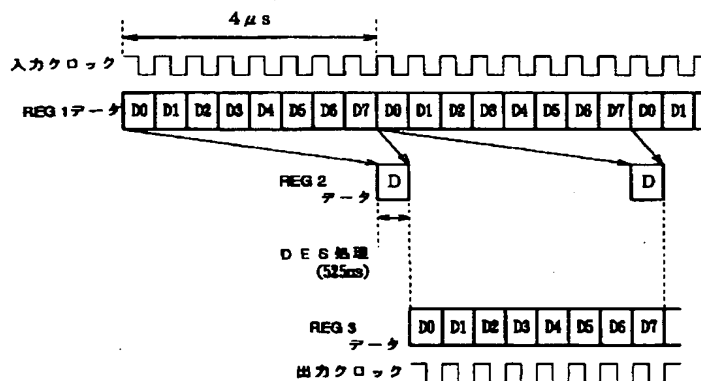
【図8】

実施例におけるDESの構成を示すブロック図



【図11】

実施例におけるDES実行部の処理シーケンスを説明する図



【図12】

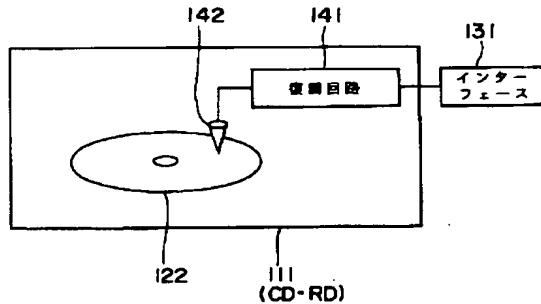
実施例のセクタ番号PID対応ポインタテーブルの内容を示す説明図

114

PID	セクタ番号
001	001 ~ 010
002	011 ~ 020
...	...
...	...

【図14】

実施例の再生装置に用いられるドライブ装置を示す図



【図15】

実施例のCD-ROM上の対応記録部の配置状態を示す図

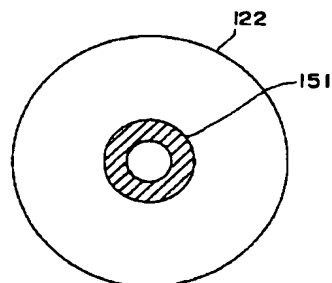
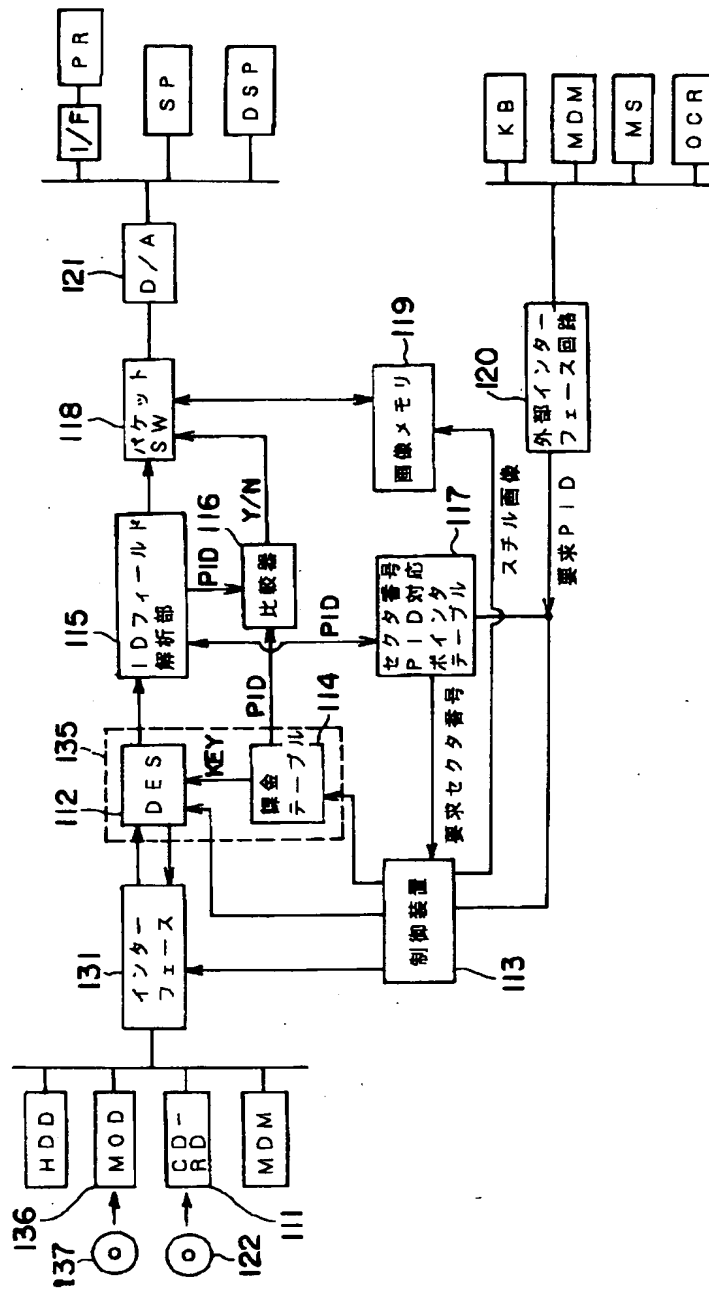
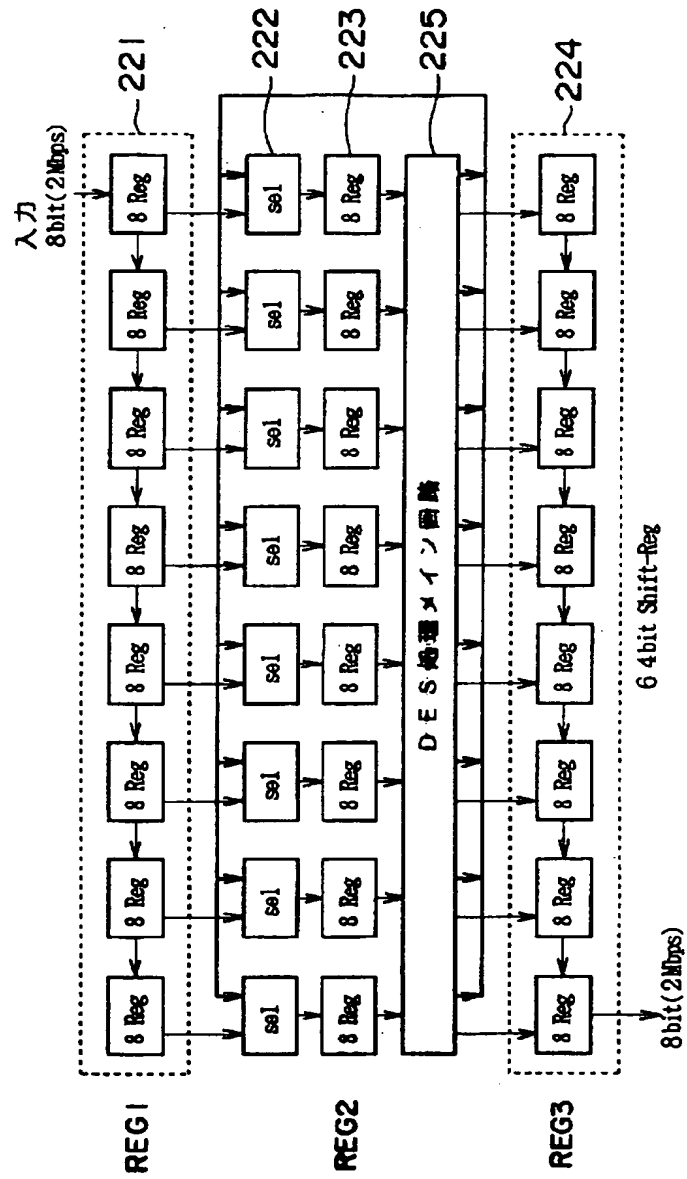


図 3 クロック再生装置の構成を示す圧縮符号化データ例の実施例



【図10】

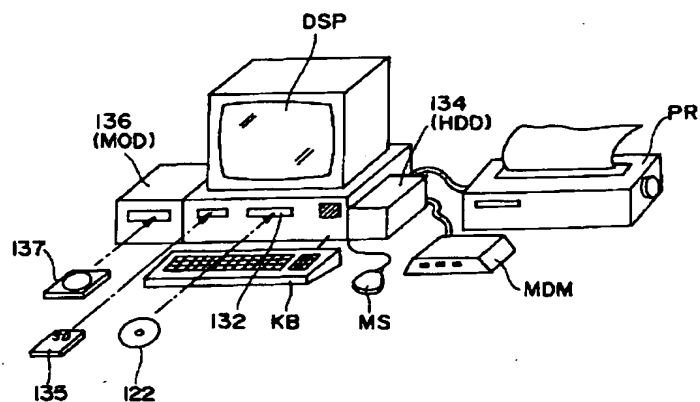
実施例におけるDES実行部の高速化を図るための構成を示すブロック図





【図13】

実施例の再生装置の機器構成を示す説明図



フロントページの続き

(51) Int. Cl. 6

H04L 9/32

// H03M 7/30

識別記号

庁内整理番号

8842-5 J

8842-5 J

F I

H04L 9/00

技術表示箇所

611A

673E